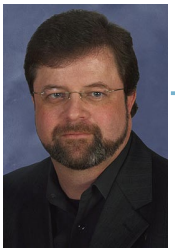
November 5, 2010

Build Security Into Your Network's DNA: The Zero Trust Network Architecture

by John Kindervag
for Security & Risk Professionals

FORRESTER® Making Leaders Successful Every Day



November 5, 2010

Build Security Into Your Network's DNA: The Zero Trust Network Architecture

by John Kindervag
with Stephanie Balaouras and Lindsey Coit

EXECUTIVE SUMMARY

This report is a deep dive into a potential way in which you could use the concepts of the Zero Trust Model and conceivably implement them in a real-world environment. One of our goals with Zero Trust is to optimize the security architectures and technologies for future flexibility. As we move toward a data-centric world with shifting threats and perimeters, we look at new network designs that integrate connectivity, transport, and security around potentially toxic data. We call this "designing from the inside out." If we begin to do all those things together we can have a much more strategic infrastructure. If we look at everything from a data-centric perspective, we can design networks from the inside out and make them more efficient, more elegant, simpler, and more cost-effective.

TABLE OF CONTENTS

NOTES & RESOURCES

In developing this report, Forrester drew from a wealth of analyst experience, insight, and research through advisory and inquiry discussions with end users, vendors, and regulators across industry sectors.

Related Research Documents

"No More Chewy Centers: Introducing The Zero Trust Model Of Information Security" September 14, 2010

"Are Converged Infrastructures Good For IT?" May 17, 2010

"TechRadar™ For Security & Risk Professionals: Network Threat Mitigation, Q3 2009" July 22, 2009

FORRESTER'S ZERO TRUST NETWORK SECURITY REPORT COLLECTION

This is the second in a collection of reports that describe the concept, architecture, and benefits of Forrester's Zero Trust Model of information security. There is a simple philosophy at the core of Zero Trust: Security professionals must stop trusting packets as if they were people. Instead, they must eliminate the idea of a trusted network (usually the internal network) and an untrusted network (external networks). In Zero Trust, all network traffic is untrusted. Thus, security professionals must verify and secure all resources, limit and strictly enforce access control, and inspect and log all network traffic.

The Zero Trust network security report collection will consist of the following reports:

- **Concept.** This report will introduce the necessity and essential concepts of the Zero Trust Model of information security.
- **Architecture.** This report will outline the key architectural components, capabilities, and required technologies of the Zero Trust Model.
- **Case studies.** In a series of case studies, Forrester will highlight security organizations that have adopted or applied concepts of the Zero Trust Model in their environment. Included in the case studies will be a discussion of best practices and benefits.

ZERO TRUST WILL CHANGE THE WAY WE DESIGN AND BUILD NETWORKS

Trust is the fundamental problem in information security today. By changing our trust model we can change our networks and make them easier to build and maintain; we can even make them more efficient, more compliant, and more cost-effective. There are several core concepts of Zero Trust: 1) There are no longer a trusted and an untrusted interface on our security devices; 2) there are no longer a trusted and an untrusted network; and 3) there are no longer trusted and untrusted users. Zero Trust mandates that information security pros treat all network traffic as untrusted. Zero Trust doesn't say that employees are untrustworthy but that trust is a concept that information security pros should not apply to packets, network traffic, and data. The malicious insider reality demands a new trust model. By changing the trust model, we reduce the temptation for insiders to abuse or misuse the network, and we improve our chances of discovering cybercrime before it can succeed.

You Must Design The Network Of The Future From The Inside Out

Networking professionals built legacy networks from the outside in. Historically, networkers have been more concerned with infrastructure than with data, more with roads than with destinations. Network professionals built yesterday's networks at the edge, with the Internet connection, and then built inward, without regard to the placement of resources or data. The networker would start at the router and all the complex routing protocols and then move to building the switching infrastructure.

At the end of the network build, users were allowed to plug resources into that network with little regard to potential security implications.

That process is untenable today. Cyberthreats have increased, while various laws and regulations track security postures more closely than ever. Shifting traffic flows and threats are forcing changes to the way we build and operate networks. We must build tomorrow's networks securely from inception. You can use the basic concepts of Zero Trust to redesign legacy networks into modern networks so that they are compliant, secure, efficient, and cost-effective.

When Bugsy Siegel decided to build the city of Las Vegas and make it one of the world's premier and most successful tourist destinations, he built the town first and the road second. He didn't build the road first and then build Las Vegas. Unfortunately, networking professionals didn't build yesterday's networks this way; they built the network pipe first and then invited everyone to build destinations second. Today we need to build networks from the inside out: Start with the system resources and data repositories that we need to protect as well as the places where we need to be compliant, then build a network out from that. Let's protect the data first and figure out how to do the road-building — the networking — second. Building roads is easy. Security is hard.

The Traditional Hierarchical Network Is Antiquated And Not Secure

Network professionals designed the traditional hierarchical network from the outside in. If we look closely at the traditional hierarchical network, we will quickly understand why new technology and new ways of doing business (especially Web 2.0, social networks, and cloud computing) have made it antiquated. Sometimes known as the "Three-Tiered Network Architecture," this is the type of network that we most often see in current corporate environments (see Figure 1).[1] The elements found in most hierarchical networks are designed so that:

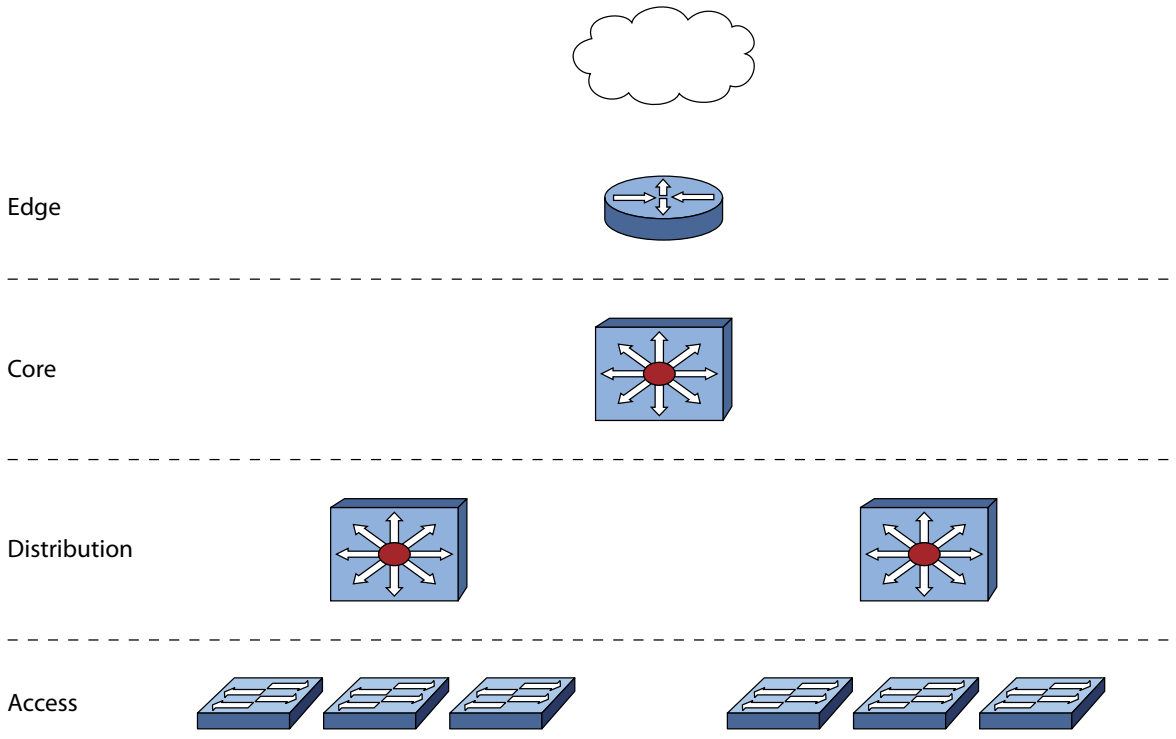
- **The core is the backbone.** The core connects the enterprise network to the Internet and aggregates all network traffic into a single high-speed, low-latency switch infrastructure. The core begins the process of sending packets to their destinations. It serves as a traffic cop, breaking up gridlock and directing traffic to less crowded roadways.

- **The distribution layer provides connectivity and enforces policy.** There is typically a single highly available core switch that sends packets to multiple distribution layer switches. The distribution layer was important early on in the creation of enterprise networking because the core was not yet powerful enough to process traffic down to the user, or access, layer with any speed or efficiency. Today, many networks, especially smaller ones, have collapsed the distribution and core tiers together to try to create cost savings and efficiencies in the data center network.

- **The access layer connects users to the network.** As the third tier of the traditional hierarchical network, the access layer defines the outer boundary of the local area network (LAN). Often called "closet" switches, each user device will connect directly to an access layer switch in order to access approved network resources.

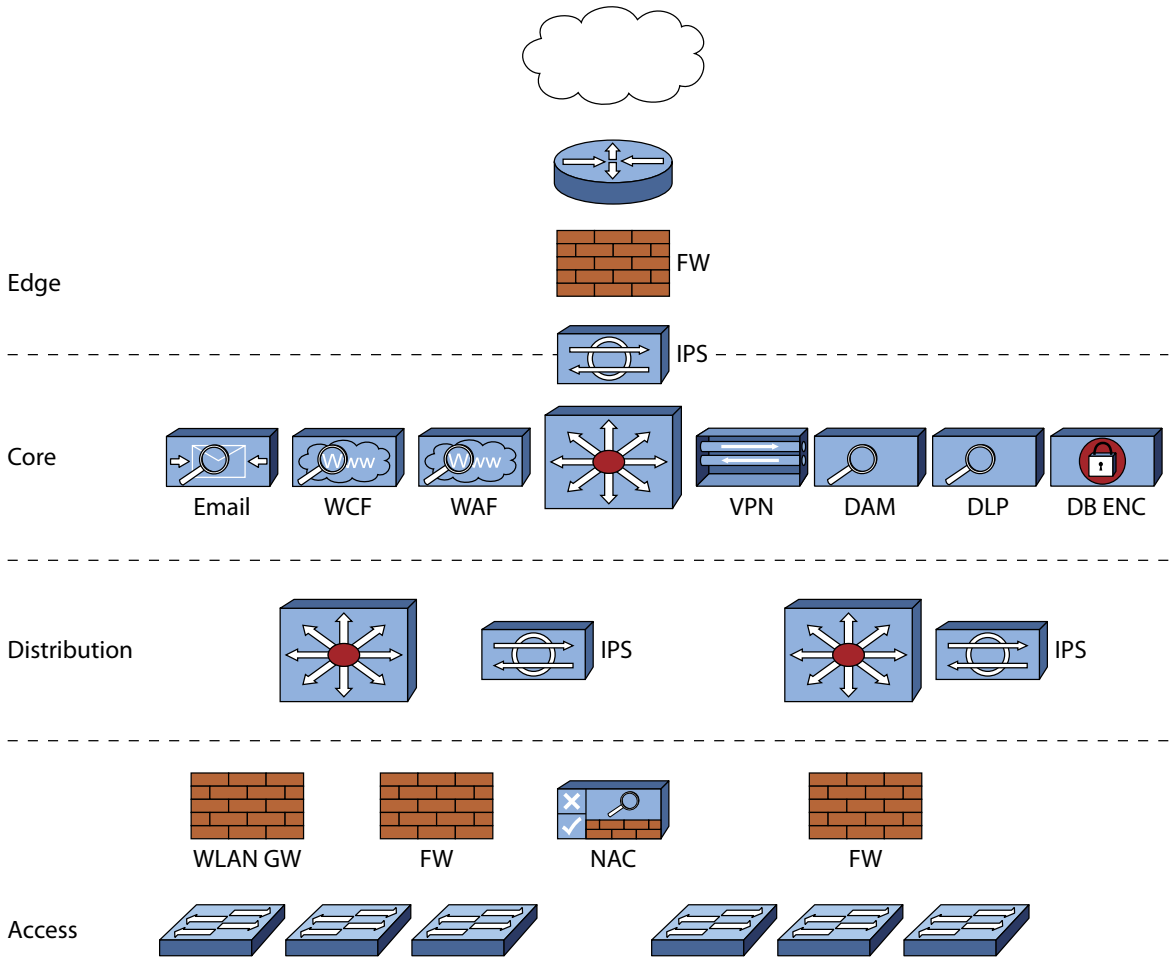
- **Security is an overlay in yesterday's hierarchical network.** There is no security layer in a three-tiered network. Network professionals downgraded or dismissed most security requirements during legacy network design. By the time they identified a security issue and brought in security professionals, network professionals had already built the network; we then had to bolt on security controls after the fact. Our networks, therefore, are overflowing with security controls wedged awkwardly into this antiquated networking model (see Figure 2). They become a management nightmare made even worse by the fact that we still have yet to fully resolve our overarching security problems.

Figure 1 Building The Traditional Hierarchical Network



57047 Source: Forrester Research, Inc.

Figure 2 Security Is An Overlay



57047 Source: Forrester Research, Inc.

USE ZERO TRUST TO REBUILD THE SECURE NETWORK

The old hierarchical network is a road built to nowhere, so when the road abruptly stopped, users just placed toxic data — credit card numbers, personally identifiable and other sensitive information — at the end of the road and walked away. This left information security professionals with the unenviable duty of cleaning up. We must redress the security implications of yesterday's networks with a new design that accounts for changing threats and new compliance realities.

Zero Trust Network Architecture Characteristics: Segmented, Parallelized, And Centralized

The Zero Trust Model of information security can embolden network designers to do unique and powerful things. It will engender infrastructure and security professionals to build security into networks by default. Current designs merely overlay existing networks with more and more controls in an attempt to create a semblance of a secure network. These efforts are generally unsuccessful because our industry is unwilling to reinvent technology that aligns with tomorrow's needs. To rethink the network requires a willingness to set aside preconceived notions about what the network should be and think about what the network could be. By taking network design down to the trust level, we can create the Zero Trust network. Zero Trust will enable security throughout your network by addressing three concepts that will empower secure networking in the future. We will design tomorrow's networks to be:

- **Easily managed and segmented for security and compliance.** Legacy networks are flat, Layer 2 fabrics. These old networks just don't function in a security-conscious environment. In the future, we need to provide easy-to-manage, segmented networks. If you're involved with almost any compliance mandate right now, you know you need a segmented network. Compliance and performance issues demand a segmented network, but hierarchical networks are difficult to segment. This is because the focus on switch fabrics and high-speed backplanes doesn't provide a way to effectively break apart the backplane for segmentation purposes.

  Some networkers advocate the use of virtual LANs (VLANs) for segmentation purposes, but they are highly insecure. Think of VLANs as the yellow line on the road. Traffic is not supposed to cross that yellow line, but there's nothing preventing a vehicle from doing so. In the same way, VLANs define a network traffic isolation policy, but they aren't technologically capable of preventing a malicious actor from moving between VLANs and gaining access to privileged information.[2] Therefore, new ways of segmenting networks must be created because all future networks need to be segmented by default.

- **Built with multiple parallelized switching cores.** The traditional switch fabric is the bottleneck that keeps us from building inherently secure and efficient networks. A unified switch fabric and massive backplane are, in fact, antithetical to multicore processing and parallelization. Once we realize that the actual problem is the very switch fabric we're so focused on, and once we start to disabuse ourselves of the notion that the network is all about the backplane, we will begin to think about networks in a completely different way. Having a several-hundred-gigabyte backplane on a core switch is of little value today because all those packets are going to different destinations, which reduces traffic efficiency.

  Modern laptops have multicore processors. If we use laptops as an example of distributed processing in which the OS provides centralized management, we can extrapolate that model to the network. This will allow designers to break the core switch into multiple smaller and

less expensive cores to take advantage of concepts such as data parallelization, thereby creating significant processing and cost efficiencies. By using the concept of parallelization inherent in multicore technology, we can create numerous different microswitch fabrics that will efficiently process specific types of packets.

- **Centrally managed from a single console.** In the early command-line days, centralized device management was not practical or possible. The prevailing solution was to combine numerous switches into a single chassis that shared the same backplane so that networking professionals could manage all the switches from a single device. Unfortunately, this creates traffic congestion as all types of traffic are shoved onto the same road, regardless of destination. We don't have to have all traffic aggregated together on the same backplane any longer. The idea of a massive backplane was created by a need to improve management. Central management of all networking elements is the key to creating the network of the future. In tomorrow's network, the centralized management solution becomes the network backplane.

Zero Trust Network Architecture Components: Microcores And Perimeters

We must strip away yesterday's hierarchical network so that security is no longer merely an overlay but is built into the DNA of the network itself. We're overburdened with individual security controls deployed in a seemingly haphazard manner. The Zero Trust network architecture is a theoretical adaptation of the Zero Trust Model of information security.[3] Not all of the technology and components described below are available today — at least not yet. While you can't go out and simply buy a Zero Trust network, you can use the architectural design components of Zero Trust to help you get past today's biases about how we should build networks and begin looking at network design from a new point of view. It will also help you better evaluate vendors, their strategy, their existing products, and their future road maps. Do they align with Zero Trust? Will they enable Zero Trust? Here are the key architectural components of Zero Trust:

- **Use an integrated "segmentation gateway" as the nucleus of the network.** Current networks rely on numerous security devices and controls to protect the network and its data. These include firewalls, IPS, WAF, NAC, content filtering gateways, network access control, VPN gateways, and other encryption products.[4] For this future-state network, Forrester envisions the development of a new product category called a network segmentation gateway (SG). This takes all of the features and functionality of individual, standalone security products and embeds them into the very fabric of the SG. By embedding a packet-forwarding engine, we have a device that can sit at the very center of the network. The SG's larger value lies in its ability to properly segment networks in a secure manner and build security into the very DNA of the network. This is a pretty radical concept, because although it takes some of its inspiration from traditional unified threat management (UTM) designs, an SG takes embedded security to the next level (see Figure 3).

A UTM is a perimeter control. An SG becomes the nucleus of the network. To be successful, a segmentation gateway would need to be very high-speed, support multiple 10 Gig interfaces, and have the ability to provide QoS or packet shaping to maintain performance. As hardware components such as network processors and other silicon drop in price and increase in speed, it's not inconceivable that vendors can tune their existing devices to function much like the SG Forrester envisions. Vendors such as Palo Alto Networks, Xceedium, Fortinet, Crossbeam Systems, and SonciWALL all have innovative, high-speed products that are poised to function as segmentation gateways.

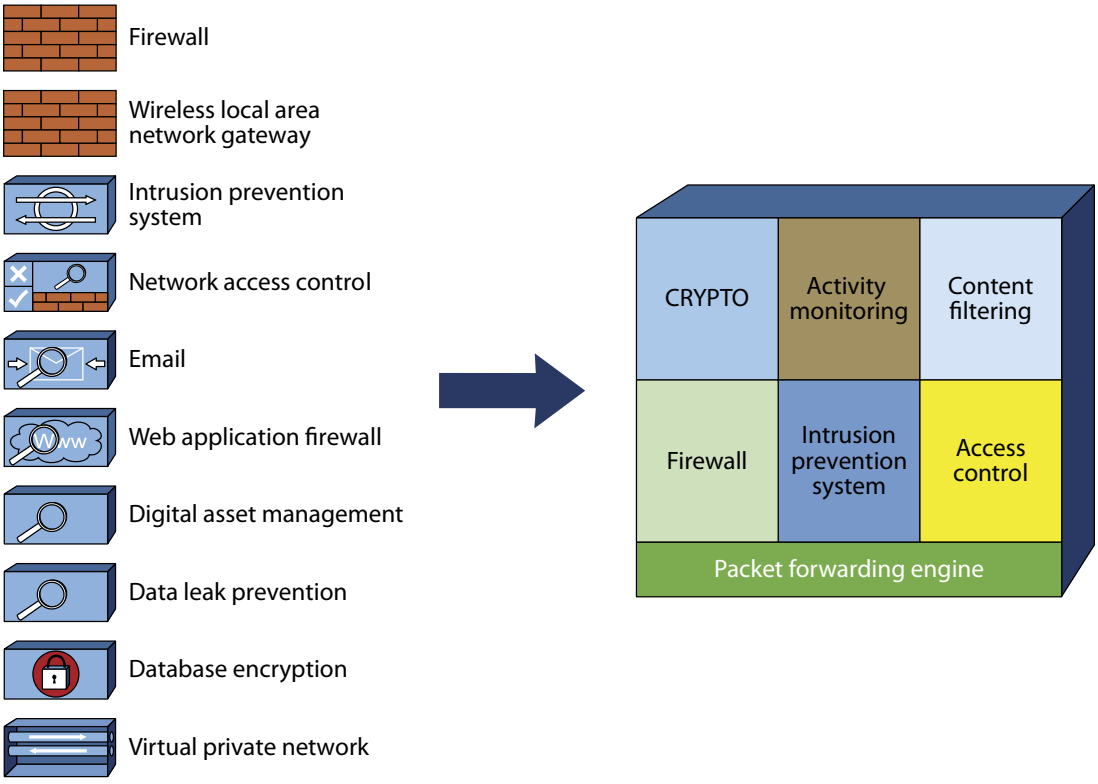
- **Create parallel, secure network segments.** A segmentation gateway defines global policy and would require multiple high-speed interfaces. This embeds security into the segmentation gateway fabric. In the Zero Trust network, each of the switching zones attached to an interface is called a "microcore and perimeter" (MCAP) (see Figure 4-1). Each segmented zone is its own microcore switch, and you can consider each zone as a microperimeter because all the resources within a specific microcore share similar functionality and global policy attributes. You centrally manage all MCAPs by aggregating all the switches within all the MCAPs into a unified switching fabric.

- **Think of centralized management as the network backplane.** In the Zero Trust network, security is the nucleus of the system, with the switch fabric placed around the central security element — the segmentation gateway. This is antithetical to the hierarchical network, where the switch infrastructure is at the center of the network and security professionals are forced to try to wedge adequate controls on top of an inflexible fabric. In the Zero Trust network, the backplane is defined by the transparent and unified management of all MCAPs (see Figure 4-2). We must move from command-line management of individual elements to a centralized intuitive management system that empowers our IT staff to easily manage expensive networks. Juniper Networks has rebuilt its management software, and its Junos Space offering can centrally manage Juniper's switches and security devices. EMC Ionix Network Configuration Manager is a standalone software platform that can manage network devices from multiple vendors to create this new management backplane.

- **Create a data acquisition network to gain complete network visibility.** An essential concept of Zero Trust is that you must inspect and log all traffic to and from each MCAP (see Figure 5). To facilitate this, Forrester is proposing the creation of a new type of network called a "data acquisition network" (DAN). Today, numerous types of networks exist: local area networks (LANs), metropolitan area networks (MANs), wireless LANs (WLANs), and wide-area networks (WANs). To enforce Zero Trust, you should consider creating a DAN. A DAN facilitates the extraction of network data — typically, packets, sylog, or SNMP messages — to a single place where you can then inspect and analyze it in near real time. A DAN is an attractive concept; anybody who's had to troubleshoot networks knows how hard it is to capture packets in a network effectively. Because all traffic traverses the segmentation gateway, which interconnects

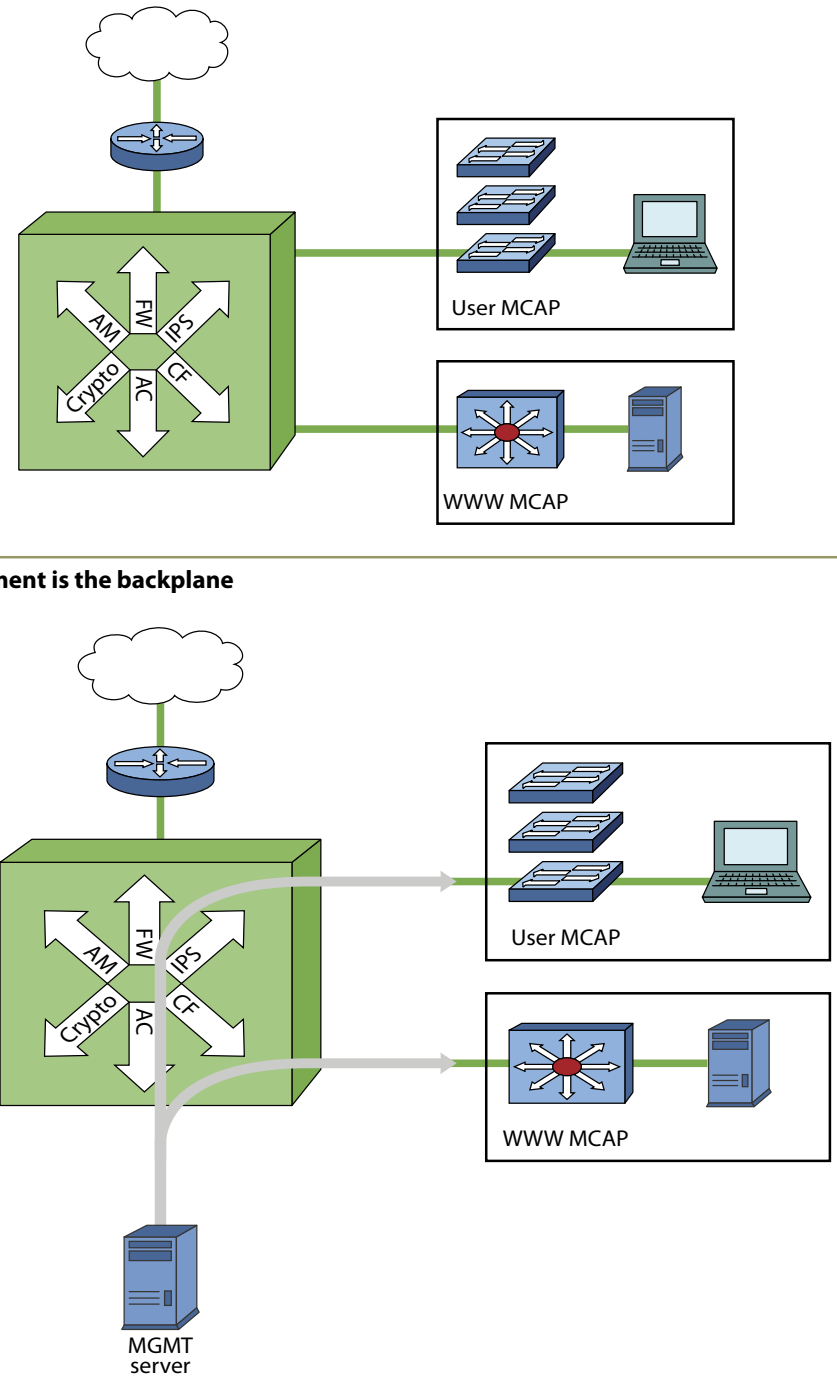
all MCAPS, data acquisition can be accomplished efficiently. All of this traffic can be mirrored and forwarded to a DAN MCAP where security information management (SIM) and network analysis and visibility (NAV) tools centrally capture, analyze, and log all traffic traversing the network. NAV, along with traditional SIM tools, provides a type of network omniscience that is imperative in today's threat environment. Cutting-edge NAV tools such as PacketMotion, Narus, netForensics, Lancope, and Lumeta will finally find their home in the DAN.

Figure 3 Rebuilding The Secure Network



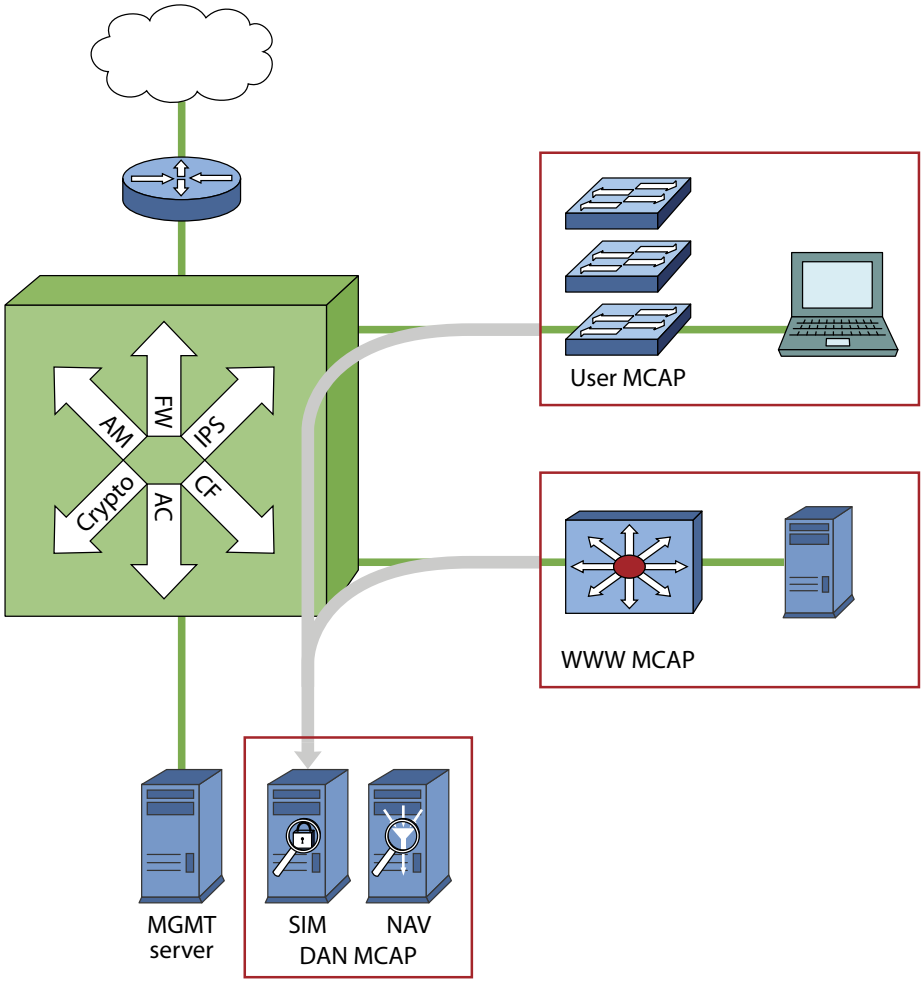
57047 Source: Forrester Research, Inc.

Figure 4 Zero Trust Network Architecture



57047 Source: Forrester Research, Inc.

Figure 5 All Traffic Is Inspected And Logged



57047 Source: Forrester Research, Inc.

THE ZERO TRUST NETWORK IS POISED TO TRANSFORM ENTERPRISE NETWORKING

Twenty-first-century networks don't work like they should. Science fiction movies and TV shows have embedded a vision of what the future should look like, but the networking industry hasn't kept pace. The processes for building, managing, maintaining, and securing a network are done in a similar manner as they were in the 1990s. Why is that? What needs to be done to make things more intuitive, more automatic, more point-and-click? The moving of packets from Point A to Point B can't be allowed to be rocket science because there are not enough rocket scientists. To fulfill expectations of the future, networks need to be simpler and easier to manage. Networks must become more intuitive and inherently secure.

Zero Trust is an opportunity to reinvent the network and create secure networking. Now is the time to begin thinking about implementing Zero Trust. There are numerous benefits implicit in the Zero Trust network, including the following:

- **It's platform-agnostic.** The Zero Trust network can support any type of resource. MCAPs provide global policy and are designed to handle a specific type of traffic. You can place a Linux server or Unix mainframe in the same MCAP as a Windows server as long as all those servers are processing the same types of traffic. For example, if you deploy a Web-facing MCAP, any Web server can be deployed within it. The segmentation gateway will control policy so that only Web protocols such as HTTP or HTTPS can traverse the MCAPs interface (see Figure 6).

- **It will reduce the cost of compliance and other security assessments.** You must segment tomorrow's network. Again using PCI compliance as an example, it's clear that one of the most effective ways of meeting PCI compliance requirements is to limit the scope of PCI via network segmentation. This implicitly demands that you segment cardholder data (CHD) from the rest of your network. Since you can create a dedicated MCAP just to hold CHD, you simplify compliance and reduce the costs of assessments.[5] A CHD MCAP will have its own set of switches and its own perimeter built into the network, so when you perform your PCI assessment, the CHD MCAP will be the only area of the network that the QSA will need to review.

- **It enables secure virtualization.** Today we must try to segment networks in order to make them compliant with a myriad of burdensome regulations, yet virtualization and segmentation are often at odds with each other. In an era of increased compliance obligations, it's extremely important that IT not deploy certain virtualized critical resources in the wrong part of the network, where they might bring an organization out of compliance with a specific data security regulation. Virtualization wants a huge Layer 2 network that makes the movement of virtual machines (VMs) easy. Zero Trust enables virtualization because it creates specific Layer 2 MCAPs that are segmented from everything else (see Figure 7). It aggregates similar types of VM hosts, and then it secures those VMs by default through segmentation gateway policies.

In the Zero Trust network, if an administrator tries to add a VM into an MCAP where it doesn't belong, that VM will not function. For example, if someone spins up a virtual instance of a database server within a Web server MCAP, that database server will not receive any traffic since the default policy for the interface attached to the Web MCAP only allows Web traffic to pass. In this instance, our security risk is minimized because SQL traffic will not be allowed to traverse the interface.

- **It will help you achieve compliance.** PCI compliance, for example, mandates that wired and wireless networks be separated by a firewall. The Zero Trust network is inherently compliant because each MCAP is a separate microperimeter where a policy is enforced (see Figure 8). This policy will often support a specific compliance requirement. In this case, the firewall embedded in the fabric of the segmentation gateway ensures that wireless access points can't be bridged directly to a core network switch, which is a significant problem in many enterprise networks and the issue that this specific PCI requirement was designed to address.

- **It will scale with your organization and new ways of doing business.** The Zero Trust network architecture is modular, and you can add MCAPs as needed. Additionally, you can add resources within an MCAP just by adding switch capacity. This doesn't add additional management burden because management is the backplane in the Zero Trust network. Because the focus is on management in Zero Trust, you can mingle large and small switches throughout the network based on port-density needs (see Figure 9). This means that companies will no longer need to overinvest in large switches just to get some semblance of device management. Size the switch to the MCAP. This means that you can use less expensive switches in smaller MCAPs, thus helping you reduce overall capital costs.

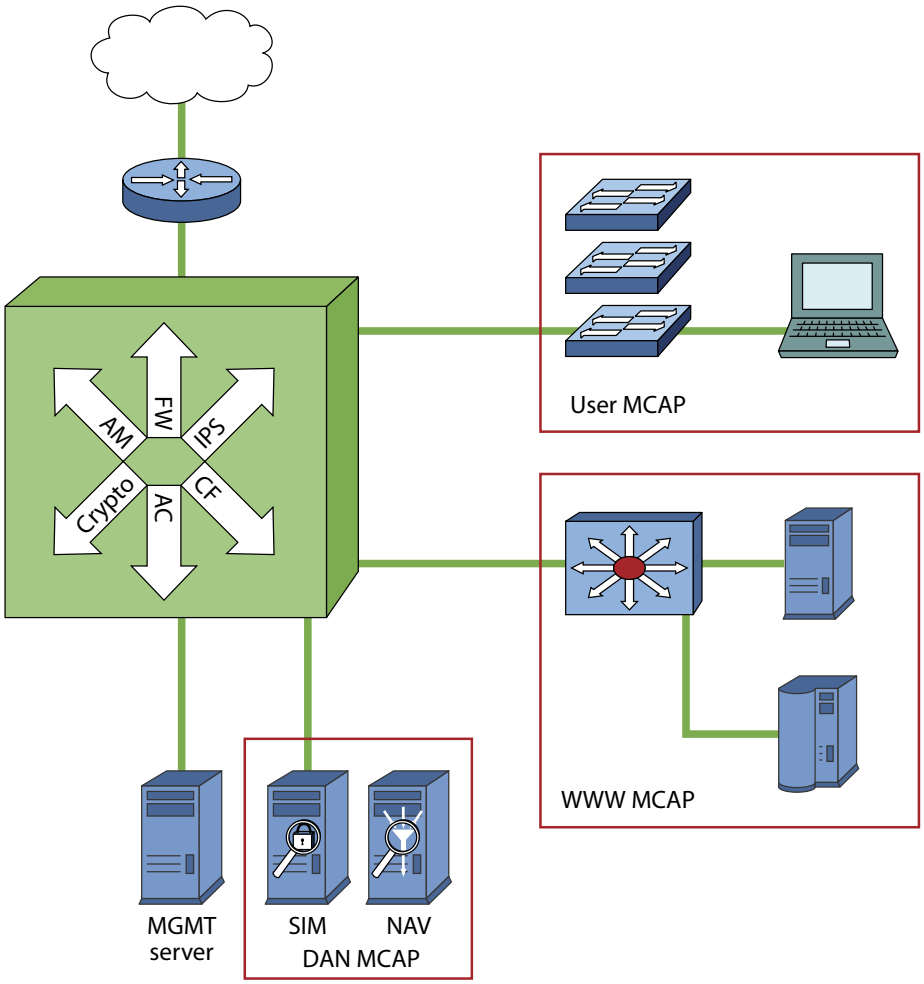
- **It's the foundation for a secure multitenant environment.** Cloud computing is all the rage. But given the difficulty in securing a hierarchical network in an enterprise network, can we really expect that a hierarchical network inside a cloud could even begin to be secure, given the challenges of transport and multitenancy? The Zero Trust network fits, by default, into a cloud or SaaS strategy. Zero Trust is natively segmented, which enables multitenancy more easily (see Figure 10). Additionally, IT could deploy virtualized instances of the segmentation gateway fabric on a single hardware cluster, with each virtual segmentation gateway (VSG) serving a specific client in a multitenant cloud environment.

- **It allows you to balance workloads easily.** You can substitute a load-balancing switch for a traditional switch within a Web MCAP. Zero Trust will require a rethinking of centralized network management solutions so that you can configure and control this load-balancing just like any other switch. The load balancer then becomes part of this aggregated backplane. This flexibility will force network management into the 21st century and enable device interoperability and lower operational costs (see Figure 11).

- **It's extensible and offers choice.** The individualized switch fabrics within an MCAP are modular. You can stack switches to allow for traffic-driven expansion of any particular traffic segment. Also, you're not locked into the features and functions of the SG. You can still use best-of-breed controls for the Zero Trust network. For example, you can augment the WAF capability of an SG by adding a standalone WAF to an MCAP at the SG interface connection (see Figure 12).

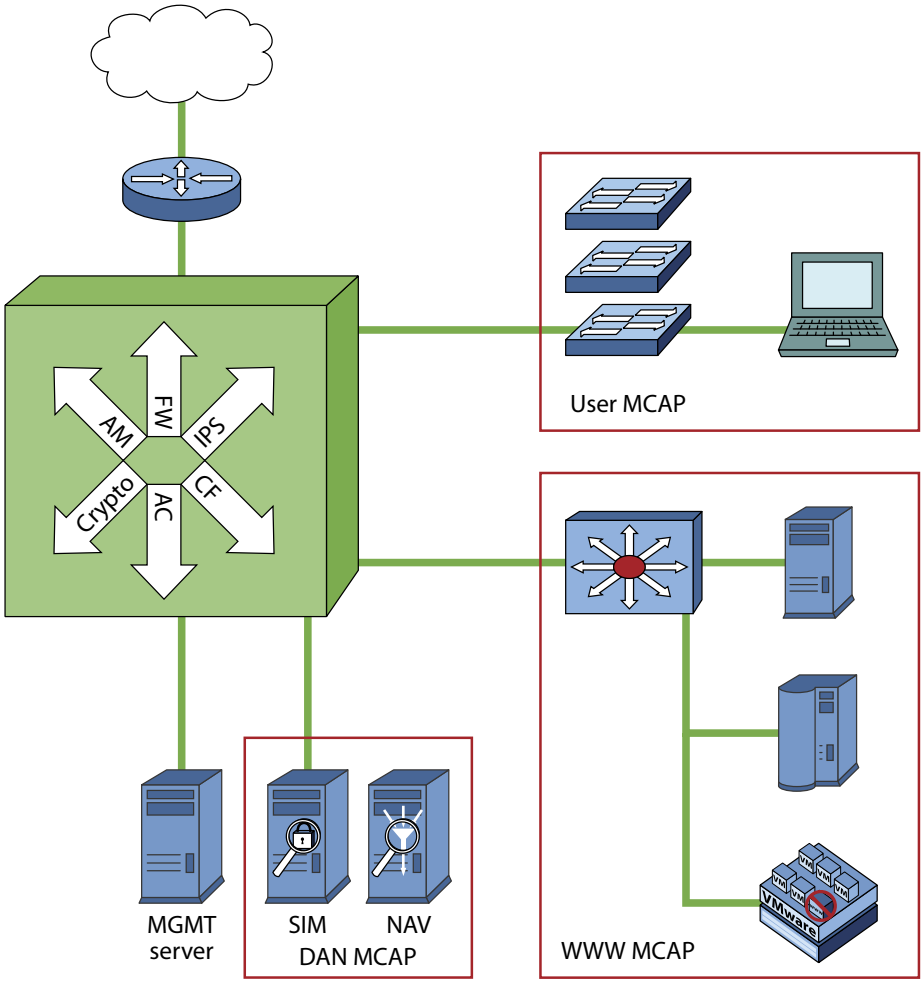
- **It can augment your existing hierarchical networks.** You can add a Zero Trust network to a current network (see Figure 13). Again, compliance may play a role here. The modularity of Zero Trust networking allows you to create a subset of your network and attach a smaller Zero Trust network to your existing network to facilitate the creation of a segmented, compliant subnetwork. For PCI, you could build a smaller PCI-compliant CHD Zero Trust network and attach it directly to your existing network. For example, we might create a Zero Trust network specifically as a cardholder network. Within our PCI compliance initiative, this might mean we need to create a segmented wireless MCAP and a segmented cardholder data MCAP. With Zero Trust networking concepts we can create a compliant and segmented network with relative ease compared with the other ways we segment networks today. Once you build a Zero Trust subnetwork, you will be able to extend it later on, and, over time, replace your existing infrastructure in manageable chunks with a Zero Trust network.

Figure 6 Zero Trust Is Platform-Agnostic



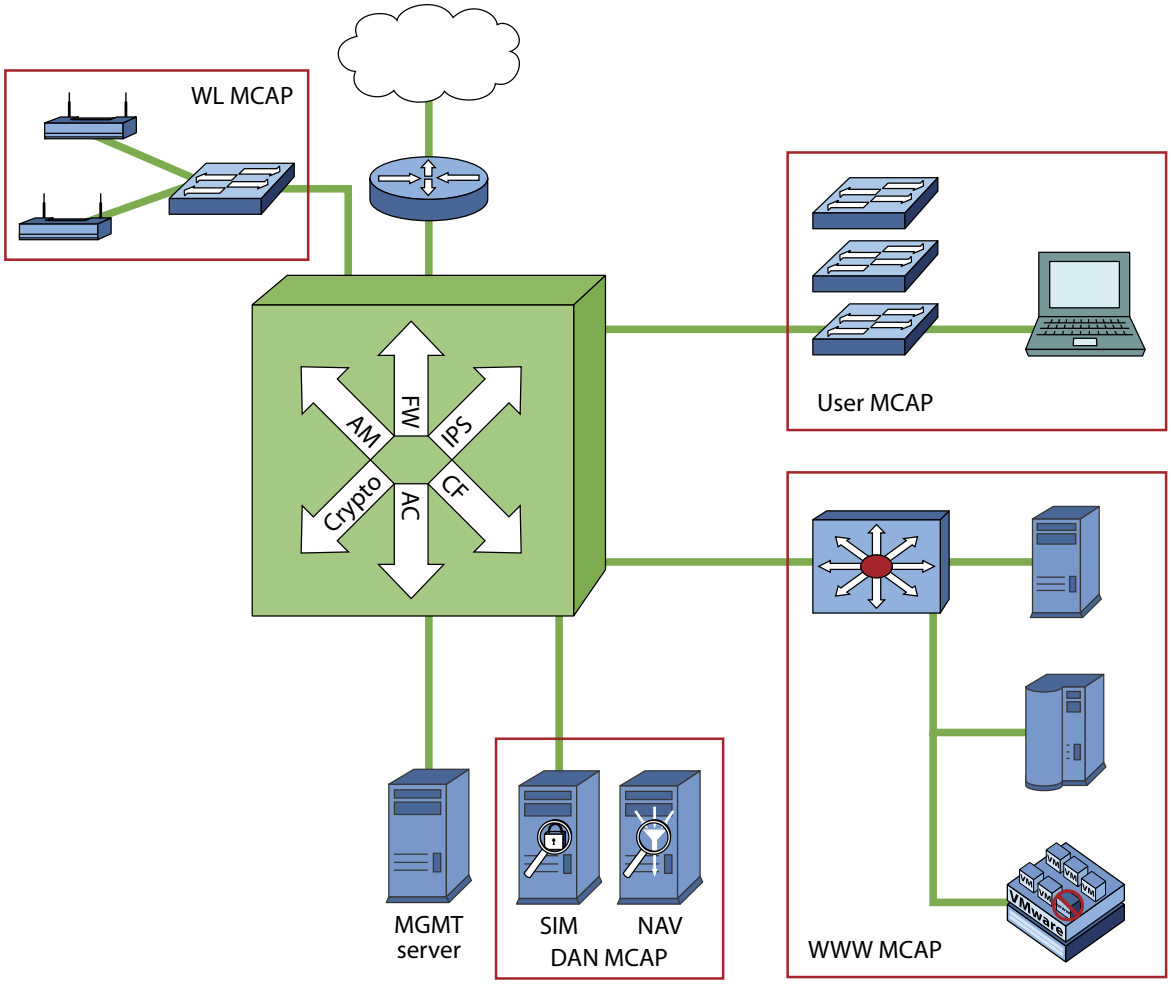
57047 Source: Forrester Research, Inc.

Figure 7 Zero Trust Enables Virtualization



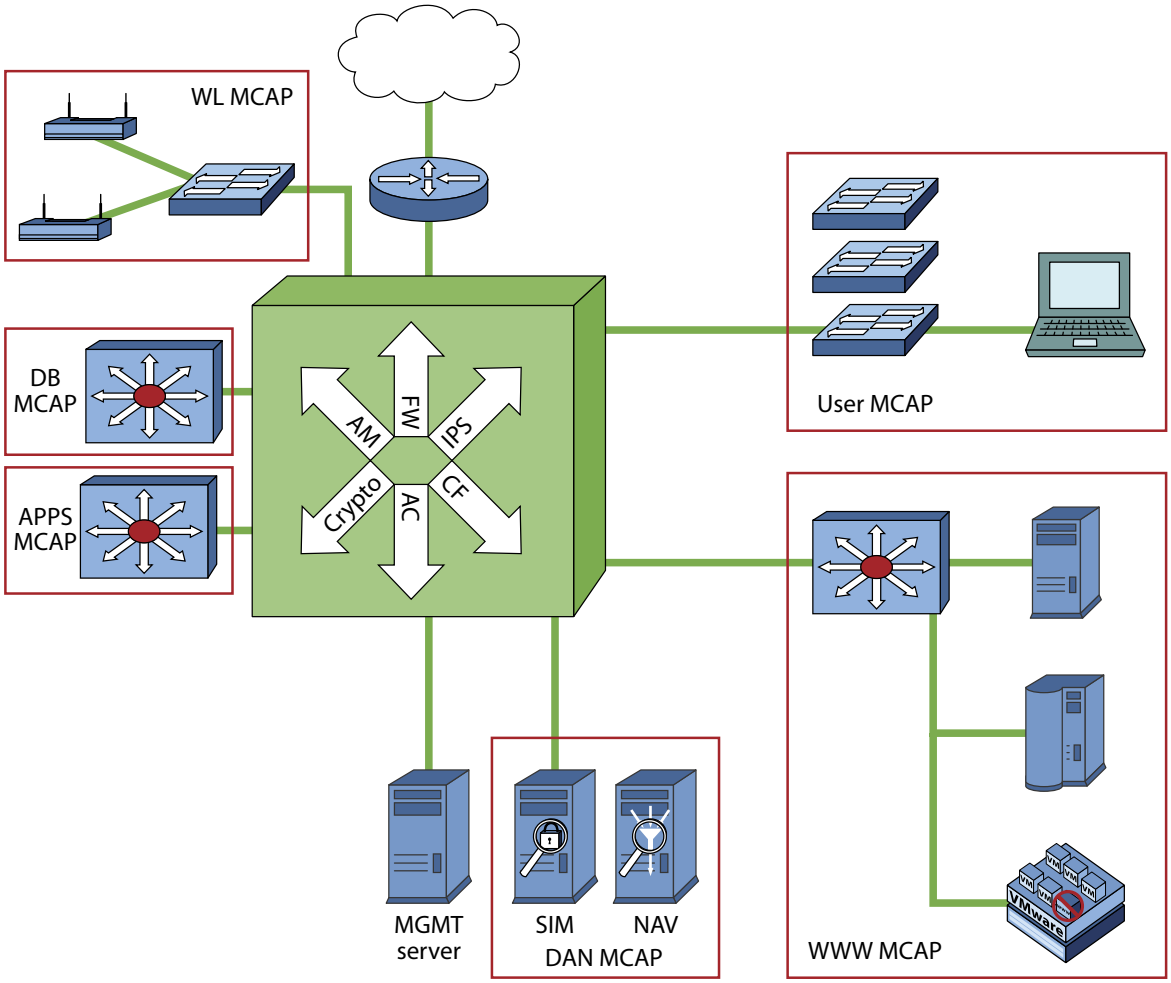
57047 Source: Forrester Research, Inc.

Figure 8 Zero Trust Network Architecture Is Compliant



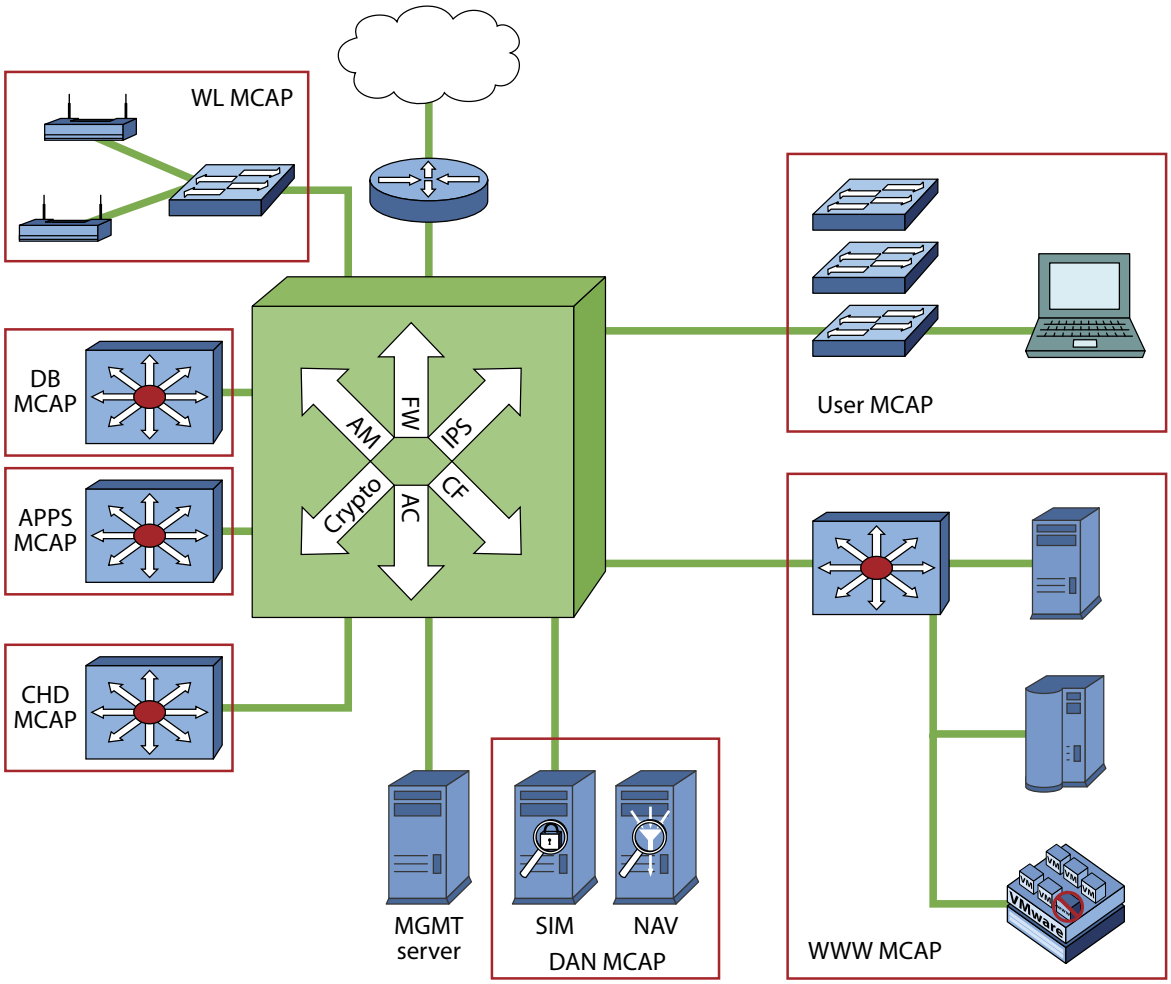
57047 Source: Forrester Research, Inc.

Figure 9 Zero Trust Network Architecture Is Scalable



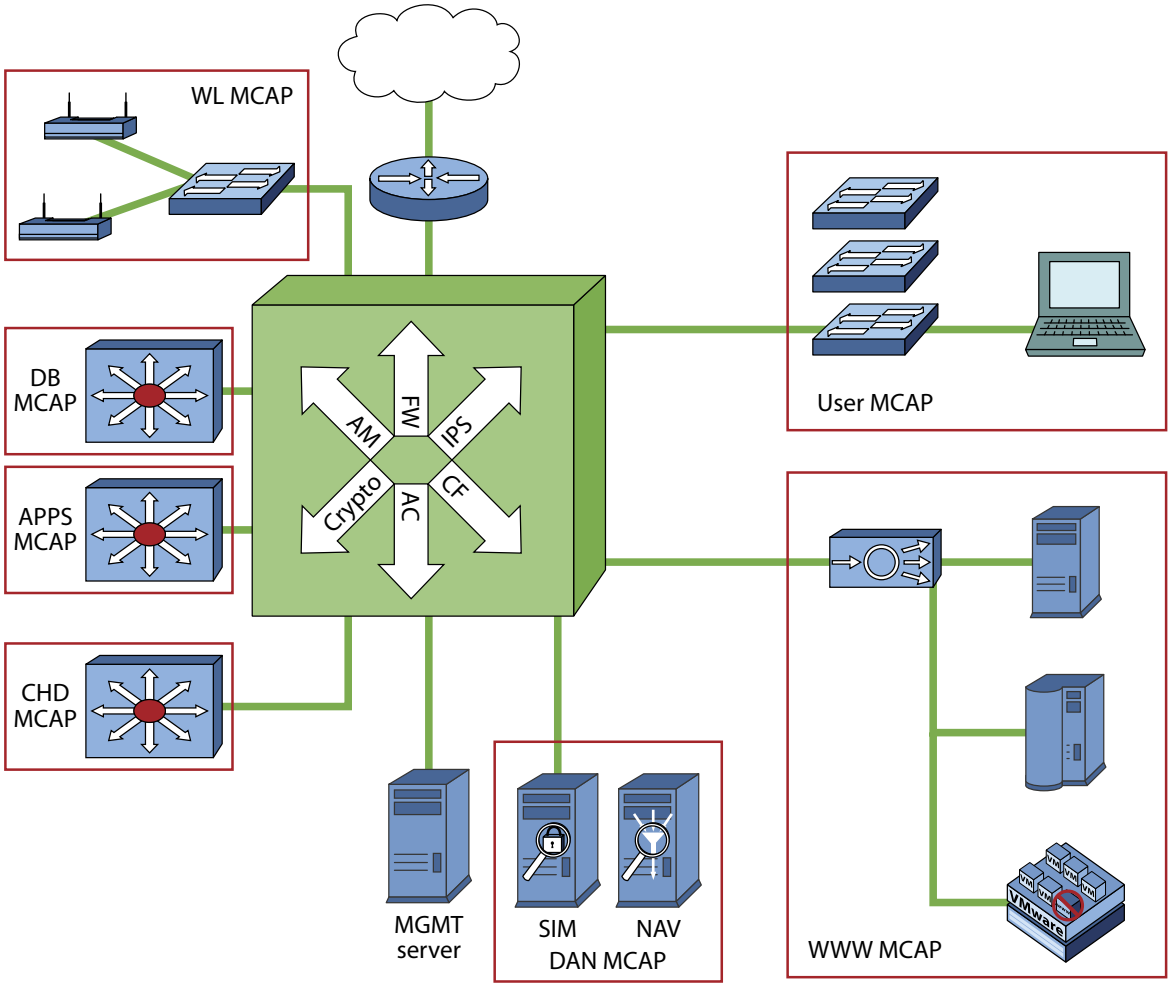
57047 Source: Forrester Research, Inc.

Figure 10 Zero Trust Network Architecture Is Segmented



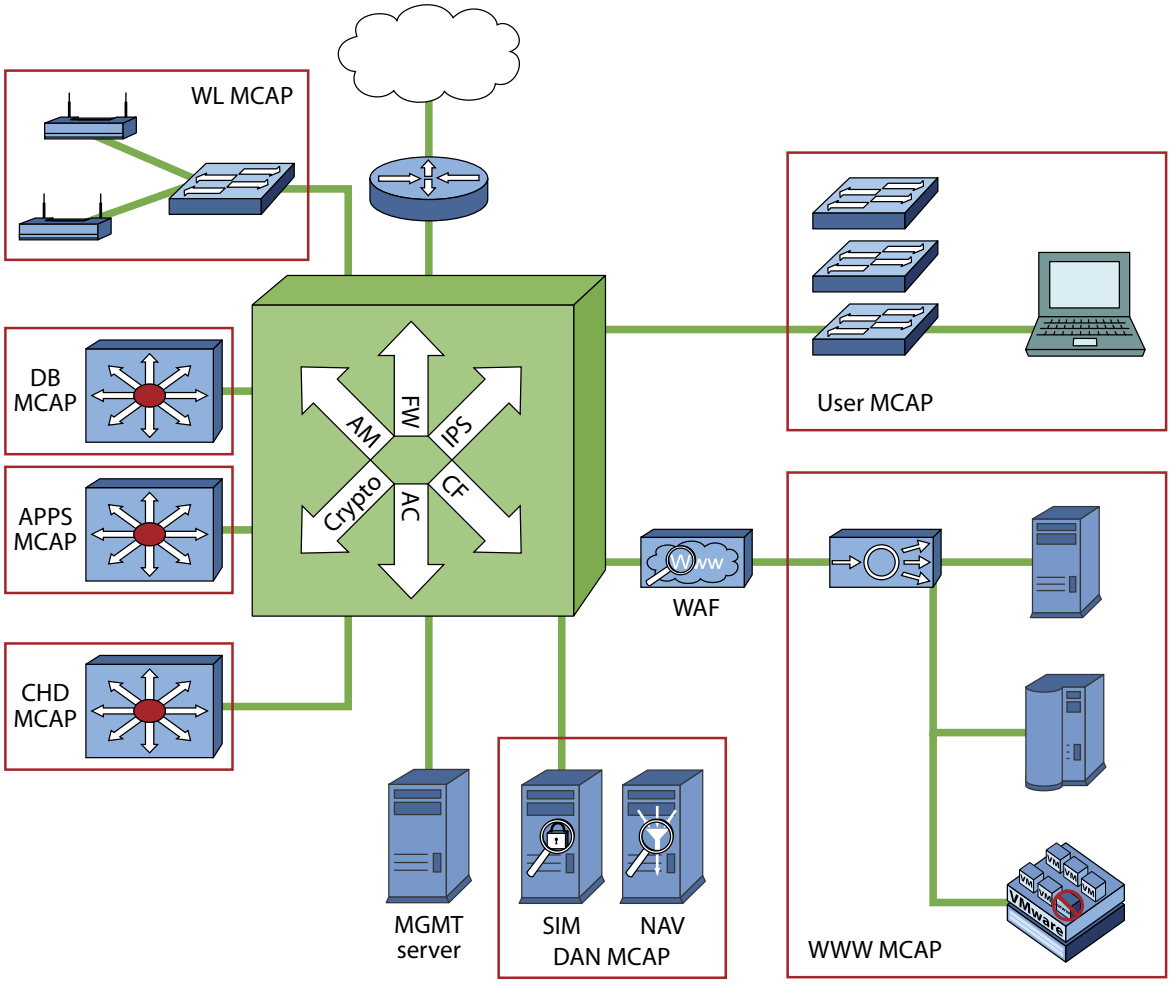
57047 Source: Forrester Research, Inc.

Figure 11 Zero Trust Network Architecture Is Flexible



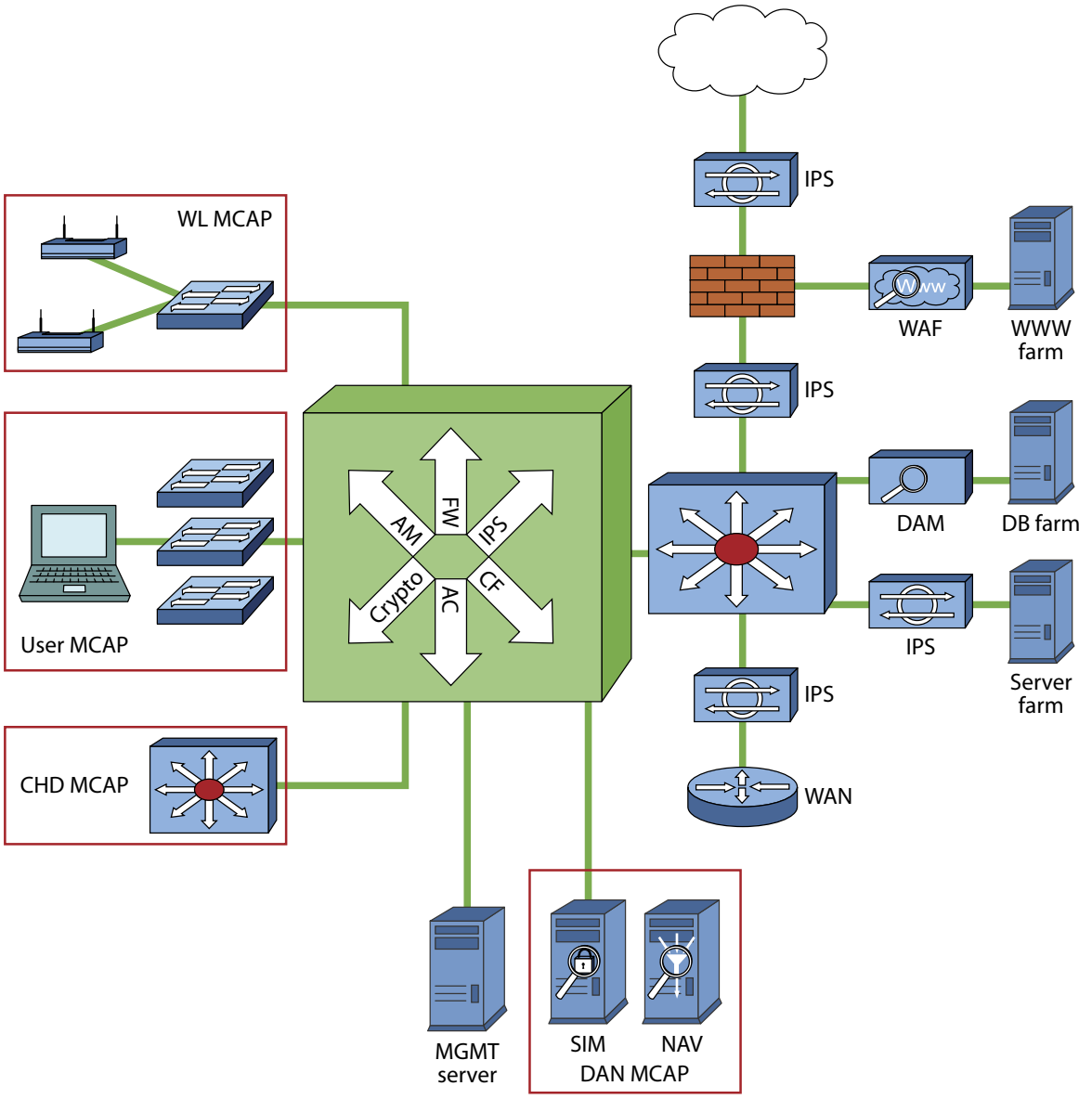
57047 Source: Forrester Research, Inc.

Figure 12 Zero Trust Network Architecture Is Extensible



57047 Source: Forrester Research, Inc.

Figure 13 Augment Hierarchical Networks With Zero Trust



57047 Source: Forrester Research, Inc.

IT PROFESSIONALS WILL UPGRADE THE NETWORK SOON — YOU NEED TO BE BY THEIR SIDE

IT and networking professionals now find themselves at an inflection point, where technologies such as unified communications, 10 GbE, and the bandwidth gluttony of Web 2.0 are converging to create new challenges for an already overburdened network. IT professionals are struggling to determine what to do to solve these unanticipated challenges. Networking has been a static pursuit for a long time. We appear to on the cusp of a networking refresh cycle, however, with an opportunity to create a new type of network: the Zero Trust network.[6] Network refresh drivers include:

- **An immediate need to segment networks for compliance and performance purposes.** An increasing number of Forrester clients are talking to us about their struggles to segment their networks. Many are now reviewing existing infrastructures with plans on segmentation redesigns in the near future.

- **A demand to support an ever-increasing number of virtualized resources.** Virtualization has great benefits, but it comes with a price. It's very easy to move VMs around the network, too easy from a security perspective. The Zero Trust network secures VMs by default. It aggregates resources so that we don't have to worry about people deploying assets in places that they shouldn't be deployed.

- **A requirement to meet the 10 GB performance expectations of users and applications.** New technologies and user expectation are straining legacy networks. As soon as we start adding more and more packets we must think about networking in a different way. Will our old networking model work? Networking professionals designed it when we had 10 Mb networks — not 10 GB networks. When Model T's were the only car, we had a different kind of road than we do today. New automotive technology meant rethinking how we built roads. As cars became faster and faster, the need to create a new type of road — the autobahn and the interstate highway — became readily apparent. New cars, new engines, and new tires redefined the way roads were built. The same must happen in networking. Fast traffic requires new networks.

- **The adoption of bandwidth-intensive unified communications.** As VoIP and IP videoconferencing become more pervasive, they open up new avenues of attack and consume extraordinary amounts of bandwidth.[7] Many legacy networks can't properly support the massive demands of unified communications on their current networks. As a result, many networking professionals are looking to replace infrastructure to support voice and video needs.

- **The adoption of converged infrastructures.** As converged networks and infrastructures begin to arrive in the data center, new challenges will arise for both infrastructure and security professionals. Security is often overlooked in current discussions about converged networking. If a converged network becomes a black box, how will we even get to its base elements to secure it? Security must be built into the black box that is the converged network using an approach like Zero Trust. Vendors can embed Zero Trust concepts into converged networks. By adding a

segmentation gateway to a converged networking device, vendors will be able to alleviate many of the concerns security professionals have with the converged networking concept, open up new market opportunities, and attract security-conscious customers. In fact, a Zero Trust-enabled converged networking solution would be especially appropriate for remote office and SMB use.[8]

It's critical that information security professionals partner with their counterparts in IT and networking infrastructure to design a network that incorporates key concepts, characteristics, and architectural components of Zero Trust. If we miss this opportunity today, we may have to wait another five to 10 years for another network architectural refresh of this magnitude, continuing meanwhile to cobble together a plethora of security controls in the hope that it makes us a bit more secure.

RECOMMENDATIONS

TODAY IS A GOOD DAY TO TAKE ACTION ON ZERO TRUST NETWORKING

The empowered enterprise technologies, including Social Computing, Web 2.0, mobile, video, and cloud, have radically changed the traditional concept of the perimeter. The Zero Trust network makes difficult concepts such as deperimeterization actionable. This architecture provides a long-term road map to a flexible, scalable, and extensible network that builds in security by default. To get started with Zero Trust today, Forrester recommends that you:

- **Change how you think about trust.** This is also a recommendation from our first report in this collection, but it bears repeating. You must challenge and break down the existing trust paradigm. You must no longer accept and espouse "Trust but verify."
- **Break away from the three-tiered hierarchical networking model.** If you were designing the network from the ground up and you didn't know about this three-tiered model, would you design your network that way? Look for greenfield subnetworks or lab environments where you can start testing and incrementally implementing Zero Trust architectural ideas.
- **Set up recurring meetings with your counterparts in networking.** Begin to socialize the Zero Trust networking concept to your networking peers. Start a cross-functional Zero Trust working group to brainstorm and whiteboard both immediate and long-term uses of Zero Trust network architecture.
- **Grill your network and security vendors about Zero Trust.** Change doesn't happen in a vacuum, and vendors must be incentivized by customer demand in order to build innovative new products that subscribe to the tenets of Zero Trust. Push your vendors so that they can provide feedback to product management and begin developing new products based on the Zero Trust Model.

- **Include Zero Trust architectural requirements in every networking or security RFP.** In a highly competitive market economy, sourcing and vendor management efforts can drive product developments. Demonstrate to your vendors that you are an educated client who cares deeply about your data and your overall security, and you will be amazed at how responsive the vendor community will become to this new model.

ENDNOTES

[1] A detailed study of traditional network design principles can be found at "Internetworking Design Basics." Source: Cisco Systems (http://www.cisco.com/en/US/docs/internetworking/design/guide/nd2002.html).

[2] For an understanding of automated VLAN attacks, read "VoIP Hopping: A Method of Testing VoIP security or Voice VLANs." Source: Jason Ostrom and John Kindervag, "VoIP Hopping: A Method of Testing VoIP security or Voice VLANs," Symantec, September 9, 2007 (http://www.symantec.com/connect/articles/voip-hopping-method-testing-voip-security-or-voice-vlans).

[3] For details about the Zero Trust Model, see the September 14, 2010, "No More Chewy Centers: Introducing The Zero Trust Model Of Information Security" report.

[4] There are numerous controls that can be used to protect networks and assets. Forrester has taken an in-depth look at the current and future state of network threat mitigation technologies. See the July 22, 2009, "TechRadar™ For Security & Risk Professionals: Network Threat Mitigation, Q3 2009" report.

[5] For a detailed discussion of network segmentation, see the July 17, 2009, "PCI X-Ray: Network Segmentation" report.

[6] Forrester believes that networkers are at a crossroads, where they are assessing the future of their current network designs and may be looking at potential redesigns. For more information, see the January 8, 2010, "Assessing Your IT Infrastructure Architecture" report.

[7] Tools such as UCSniff are available to demonstrate attacks on unified communications systems. Source: UCSniff (http://ucsniff.sourceforge.net/).

[8] IT pros have most of the basic ingredients to cook up their own cloud-like infrastructure — but there's no recipe, and many ingredients just don't combine well. Complicating the story are the traditional infrastructure silos around servers, networks, and storage that must work together in a new, truly integrated way. Vendors like Cisco, Dell, EMC, HP, and IBM know you need packaged solutions that just work, but until recently they left too much of the burden on their customers. Recent integrated solutions take a big step toward delivering complete virtual infrastructures in a box, but to effectively use them, you must assess your own virtualization maturity, start small with development and test workloads, and consider whether you really need to run it yourself. See the May 17, 2010, "Are Converged Infrastructures Good For IT?" report.

FORRESTER®

Making Leaders Successful Every Day

Headquarters

Forrester Research, Inc.
400 Technology Square
Cambridge, MA 02139 USA
Tel: +1 617.613.6000
Fax: +1 617.613.5000
Email: forrester@forrester.com
Nasdaq symbol: FORR
www.forrester.com

Research and Sales Offices

Forrester has research centers and sales offices in more than 27 cities internationally, including Amsterdam; Cambridge, Mass.; Dallas; Dubai; Foster City, Calif.; Frankfurt; London; Madrid; Sydney; Tel Aviv; and Toronto.

For a complete list of worldwide locations visit www.forrester.com/about.

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com.
We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc. (Nasdaq: FORR) is an independent research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. Forrester works with professionals in 19 key roles at major companies providing proprietary research, customer insight, consulting, events, and peer-to-peer executive programs. For more than 27 years, Forrester has been making IT, marketing, and technology industry leaders successful every day. For more information, visit www.forrester.com.

FORRESTER®